(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 January 2004 (08.01.2004)

PCT

(10) International Publication Number
WO 2004/004235 A1

(51) International Patent Classification[7]: H04L 12/28, H04Q 7/38, H04L 29/06

(21) International Application Number: PCT/US2003/020502

(22) International Filing Date: 27 June 2003 (27.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/184,750 28 June 2002 (28.06.2002) US

(71) Applicant: **WAVELINK CORPORATION** [US/US]; Suite 300, 11332 NE 122nd Way, Kirkland, WA 98034 (US).

(72) Inventors: **WHELAN, Robert, J.**; 545 Kirkland Avenue, Kirkland, WA 98033 (US). **WAGENEN, Lamar, Van**; 981 E. Diana Hills Way, Sandy, UT 84094 (US). **MORRIS, Roy**; 8812 NE 191st Place, Bothell, WA 98011 (US).

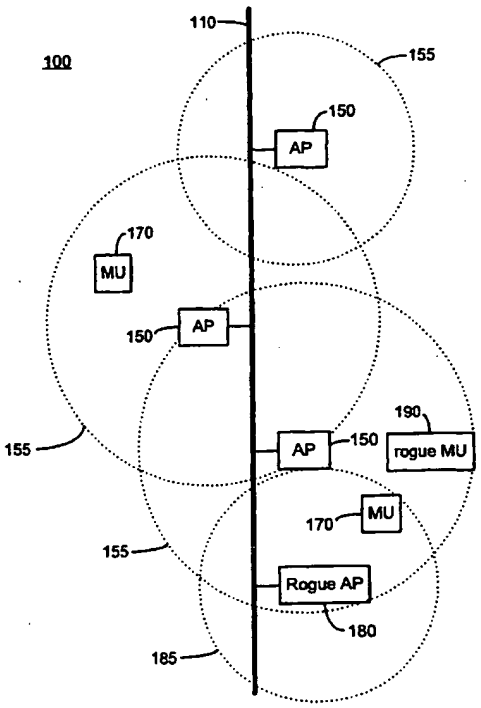
(74) Agents: **LEBOWITZ, Henry, C.** et al.; Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

*[Continued on next page]*

(54) Title: SYSTEM AND METHOD FOR DETECTING UNAUTHORIZED WIRELESS ACCESS POINTS




(57) Abstract: Unauthorized wireless access points are detected by configuring authorized access points and mobile units to listen to all wireless traffic in its cell and report all detected wireless devices to a monitor. The monitor checks the reported devices against a list of authorized network devices. If the reported wireless device is not an authorized device, the monitor determines if the reported device is connected to the network. If the reported device is connected to the network and is not an authorized device, the monitor alerts the network operator or network manager of a rogue device connected to the network and attempts to locate and isolate the rogue device.

WO 2004/004235 A1

# SYSTEM AND METHOD FOR DETECTING UNAUTHORIZED WIRELESS ACCESS POINTS

## Field of the Invention

The present invention relates to the field of communication/computer networks. Specifically, the present invention relates to increasing security of wireless networks.

## Background of the Invention

Citation or identification of any reference in this Section or any section of this Application shall not be construed to mean that such reference is prior art to the present invention.

A Wireless Local Area Network (WLAN) enables network devices to communicate with each other wirelessly, typically by radio. A WLAN typically includes a wired portion and a wireless portion. The wired portion is typically connected (for example, via a router and/or firewall) to a larger network, such as a business wide-area network, and/or the Internet.

The wireless portion of a WLAN typically includes at least one access point and at least one mobile unit. An access point is a wireless device that provides WLAN connectivity to mobile units. An access point is typically physically connected to the wired portion of the WLAN and capable of transmitting and receiving communications between a wired portion of the WLAN and a wireless portion of the WLAN. However, some access points are configured as repeaters, and lack a physical connection to a wired portion of the WLAN, instead connecting to the WLAN via another access point. As used here, a mobile unit is a wireless device (whether actually mobile or not) capable of communicating wirelessly with an access point or other device on a WLAN, and which is at least part of the time not physically wired to the wired portion of the WLAN. Mobile units generally do not provide WLAN connectivity to other mobile units. Each access point is capable of communicating with wireless devices

(e.g. 802.11 access points) use a simple bridging protocol and can be added to a compatible wired network without any centralized control or action. Moreover, many inexpensive access points are very difficult to detect once installed. Many local work groups install an access point onto the existing company network, not appreciating the increased risk to the entire network created by the newly attached rogue access point, without bothering to inform the network administrator of the rogue access point. Moreover, the rogue access point is often configured using settings such as factory default settings that do not conform to the security settings of the authorized network devices and therefore represents a serious security risk to the entire network.

Network administrators usually have at least one network management utility that is capable of discovering most of the network devices attached to the network. Almost all such utilities, however, require either a query/response between the management agent and the network device or an agent executing on the network device and reporting to the management agent. Many inexpensive access points, however, are not configured to respond to standard management queries and are therefore very difficult to detect.

Therefore, there exists a need for the detection of unauthorized rogue access points connected to a network.

## Summary of the Invention

In one aspect, the invention comprises a system for detecting unauthorized wireless access points, the system further comprising: a database of authorized wireless access points; and a server configured to receive a message from a wireless device, the message indicating the existence of a wireless access point, the server being further configured to query the database to determine whether the wireless access point is authorized.

In another aspect, the invention comprises a system for detecting unauthorized wireless access points, the system further comprising: one or more electronic data structures comprising data representing one or more mobile wireless devices operatively associated with one or more authorized wireless

In another aspect, the invention comprises a method for detecting an unauthorized wireless device on a WLAN comprising the steps of: detecting the presence of an unknown wireless device within a cell of a wireless device known to the WLAN; monitoring WLAN traffic for a message from the unknown wireless device; and classifying the unknown wireless device as an unauthorized wireless device if the monitored traffic includes a message from the unknown wireless device.

In another aspect, the invention comprises a system for securing a network, comprising: a network monitor configured to monitor a network for unauthorized access points; the network monitor being further configured to attempt to disable wireless communications via an unauthorized access point. In one embodiment, the unauthorized access point comprises a MAC address filter for prohibiting access to the access point based on information describing one or more MAC addresses; and the network monitor is further configured to set the MAC address filter of the unauthorized access point to prohibit access by any wireless device to the access point. In another embodiment, the system further comprises a switch or router configured to transfer information between at least two network segments; and the network monitor is further configured to configure the switch or router to prevent transfer of information through the switch originating from or addressed to the unauthorized access point.

In another aspect, the invention comprises a wireless security system, comprising: a wired network segment enabling communication between a first network device and a second network device via at least one wire; at least one access point electrically connected to the wired network segment configured to communicate via wireless electromagnetic signals with one or more mobile wireless devices when the one or more mobile wireless devices are within a communication zone of the access point; and a network monitor configured to disable wireless communication with the at least one access point according to a regular business schedule.

In one embodiment, the network monitor preferably determines whether reported devices are connected to the wired network by monitoring the network for packets including wireless device identification information reported by one or more wireless receivers. In a preferred 802.11 embodiment, the wireless device identification information comprises a Medium Access Control (MAC) address of the reported wireless device. By monitoring the network for the MAC address reported by the wireless receiver, the network monitor can determine if traffic from the reported wireless device is being carried by the monitored network.

When an unknown access point is detected, the network monitor preferably attempts to identify the unknown access point on the network, and to isolate the unknown access point.

In one preferred embodiment, the wireless receivers comprise authorized mobile units, which are used to listen for unknown access points and/or mobile units. Conventionally, a mobile unit is programmed to process only transmissions directed to the mobile unit. In one embodiment of the present invention, however, a mobile agent is installed on a plurality of the network's authorized mobile units and configured to process all transmissions detected by the each mobile unit on which the mobile agent executes. Preferably, the mobile agent executes even when the mobile units are not associated with an access point. The mobile agents preferably report on access point/mobile unit traffic information to the network monitor, or store traffic information for later reporting to the monitor. Reporting may be initiated by a mobile unit, or by the network monitor.

In one preferred embodiment, at least one mobile unit is capable of determining its location, via GPS for example, and includes this information in its report to the monitor. By reporting on wireless traffic, the mobile agents have a greater likelihood of detecting unknown access points or mobile units that may represent a security threat to the network. Preferably, reporting mobile units also include information identifying the access point with which the reported mobile unit is communicating, such as the BSSID of the access point, and the IP address used by the mobile unit, if any.

unit is within the access point's cell when the beacon frame is broadcast, the mobile unit may establish a connection with the access point by transmitting a probe request frame. Any rogue mobile unit within the access point's cell, however, will also hear the beacon frame and may try to access the network through the access point. Therefore, the access point may be configured to operate silently, suppressing the transmission of the BSSID and only listening for probe request frames from mobile units within the access point's cell. If the access point is configured to operate silently, the access point will listen to all probe requests broadcast in its cell, check the destination address of the request, and complete the reception of the frame if the destination address matches the address of the access point. The access point transmits a probe response to the mobile unit containing information necessary to establish communication with the access point.

Once the 802.11 mobile unit discovers an access point, the mobile unit transmits an association request frame to the access point to become associated with the access point. The access point transmits an association response frame to the mobile unit accepting or rejecting the association. If the association is accepted, the access point assigns an association ID to the association.

In one preferred embodiment, wireless devices such as mobile unit 170 are used to discover access points such as rogue access point 180 by transmitting probe requests and reporting all probe responses to a network monitor. Preferably, the network monitor is an agent executing on a machine connected to the wired portion of the network. The network monitor preferably maintains information identifying known access points and authorized access points, and optionally known mobile units.

Fig. 2 is a flowchart of one embodiment of the present invention. The network monitor receives access point identification information from a wireless receiver in step 210. The access point identification may be the BSSID of the access point (typically the MAC address), and/or another address of the access point such as the IP address. In one embodiment, a mobile agent executing on a known mobile unit hears an access point by receiving a beacon frame from the

Once the rogue access point has been verified, the monitor preferably automatically notifies the network operator or enterprise network manager of the existence of a rogue access point on the network in step 240. Notification may be accomplished via email, traps, SNMP, or other methods known to one of skill in the art.

The network monitor may also attempt to disable communications between the network and the rogue access point from the network in step 250. In one embodiment, the monitor changes the MAC address filter settings on the rogue access point to exclude all MAC addresses, effectively preventing the use on the rogue access point on the network. In another embodiment, the monitor changes the routing table settings of network devices such as routers or switches to prevent network traffic to and from the rogue access point and thereby minimize the risk to the network. The network monitor may also attempt to disable the radio of rogue access point, or to reset the rogue access point to factory default settings that are more easily managed. Other techniques, such as an echo attack, or sending connection *close* or *reset* TCP/IP messages to rogue wireless devices may alternatively be used to disable communications.

If the network monitor can verify that the access point for which identification information has been received is not connected to the wired portion of the network, the network monitor preferably updates a table comprising information of known access points that are not on the wired portion of the network. Such access points may be, for example, connected to unrelated wired networks in nearby locations. If the MAC address of an access point maps to vendor information indicating that the access point supports RARP or another protocol through which the access point could reliably be discovered on the wired portion of the network, and the network monitor tries but fails to verify that the access point is on the wired portion of the network using the reliable protocol, the network monitor may store information that the access point is not on the wired portion of the network. This technique may not work in cases where the MAC address of the access point has been forged. Moreover, some access points may be configured so that it may not be possible to reliably verify that the access point is not connected to the wired portion of the network.

searches for traffic on the wired network from the reported mobile unit in step 330, preferably by looking for the MAC address of the mobile unit on the wired portion of the WLAN. If the monitor detects network traffic from the reported mobile unit but the reported mobile unit is not part of the currently connected mobile unit list, the mobile unit must be associated with a rogue access point. The network monitor then automatically notifies the network operator or enterprise network manager of the existence of a rogue access point on the network in step 340. Notification may be accomplished via email, traps, SNMP, or other methods known to one of skill in the art.

The network monitor also preferably attempts to identify the rogue access point in step 350. The monitor preferably issues a Reverse Address Resolution Protocol (RARP) request to identify the corresponding IP address of the rogue access point. Other methods may also be used. If the rogue access point responds to the RARP request, the network monitor may also attempt to isolate the rogue access point from the network in step 250. In one embodiment, the monitor changes the MAC filter settings on the rogue access point to exclude all MAC addresses, effectively preventing the use on the rogue access point on the network. In another embodiment, the monitor changes the MAC filter table settings of network devices such as routers or switches to prevent network traffic to and from the rogue access point and minimize the risk to the network. In another embodiment, the monitor determines a port on a switch or router to which the access point is connected and disables the port.

Fig. 4 is a flowchart of another embodiment of the present invention. The network monitor receives mobile unit identification in step 410. In step 420, the monitor checks a list of authorized mobile unit to determine whether the reported mobile unit is an authorized mobile unit. If the reported mobile unit is an authorized mobile unit, the monitor returns to step 410 to receive another mobile unit identification. If the reported mobile unit is not an authorized mobile unit, the monitor notifies the network operator or enterprise network manager of the existence of a rogue mobile unit in step 430.

The network monitor may also attempt to isolate the rogue mobile unit from the network in step 440. In one embodiment, the monitor changes the MAC

the network segment), then there must exist a rogue access point on the network segment, and the network monitor notifies the operator 540. Preferably the MAC address of the access point with which the mobile unit is associated is reported by the wireless receiver, and the monitor attempts to identify the rogue access point in step 540 by using the reported MAC address to transmit RARP requests or other methods. If the rogue access point is identified the network monitor preferably attempts to isolate or disable network communications with the rogue access point as described above.

In another aspect of the invention, the network monitor is preferably configured to periodically disable wireless communications on the network, preventing all wireless communications, according to a defined business schedule. For example, if business hours at a particular location are 8 a.m. to 6 p.m. Monday through Friday, the network monitor is preferably configured to disable wireless communications at the location between 6 p.m. and 8 a.m. Monday through Friday, and all weekend. Wireless communications are preferably disabled by modifying MAC filter tables in access points connected to the network and/or modifying switch interface tables to prevent switching of packets to and from the access points. Other methods for disabling wireless communications may be used.

The invention described and claimed herein is not to be limited in scope by the preferred embodiments herein disclosed, since these embodiments are intended as illustrations of several aspects of the invention. Any equivalent embodiments are intended to be within the scope of this invention. Indeed, various modifications of the invention in addition to those shown and described herein will become apparent to those skilled in the art from the foregoing description. Such modifications are also intended to fall within the scope of the appended claims.

A number of references are cited herein, the entire disclosures of which are incorporated herein, in their entirety, by reference for all purposes. Further, none of these references, regardless of how characterized above, is admitted as prior to the invention of the subject matter claimed herein.

6. A system for detecting unauthorized access points, comprising:
a network segment for which no access point is authorized; and
a network monitor configured to detect on the network segment a message originating from a wireless device.

7. A system for detecting unauthorized access points comprising:
a wired network segment enabling communication between a first network device and a second network device via at least one wire;
an access point electrically connected to the wired network segment configured to communicate via wireless electromagnetic signals with one or more mobile wireless devices when the one or more mobile wireless devices are within a communication zone of the access point; and
a network monitor configured to receive from the access point a list of all mobile wireless devices within the communication zone of the access point and to determine the presence of an unauthorized device electrically connected to the wired network based on the list of wireless devices received from the access point.

8. A method for detecting an unauthorized wireless device on a WLAN comprising the steps of:
detecting the presence of an unknown wireless device within a cell of a wireless device known to the WLAN;
monitoring WLAN traffic for a message from the unknown wireless device; and
classifying the unknown wireless device as an unauthorized wireless device if the monitored traffic includes a message from the unknown wireless device.

9. A system for securing a network, comprising:
a network monitor configured to monitor a network for unauthorized access points;
the network monitor being further configured to attempt to disable

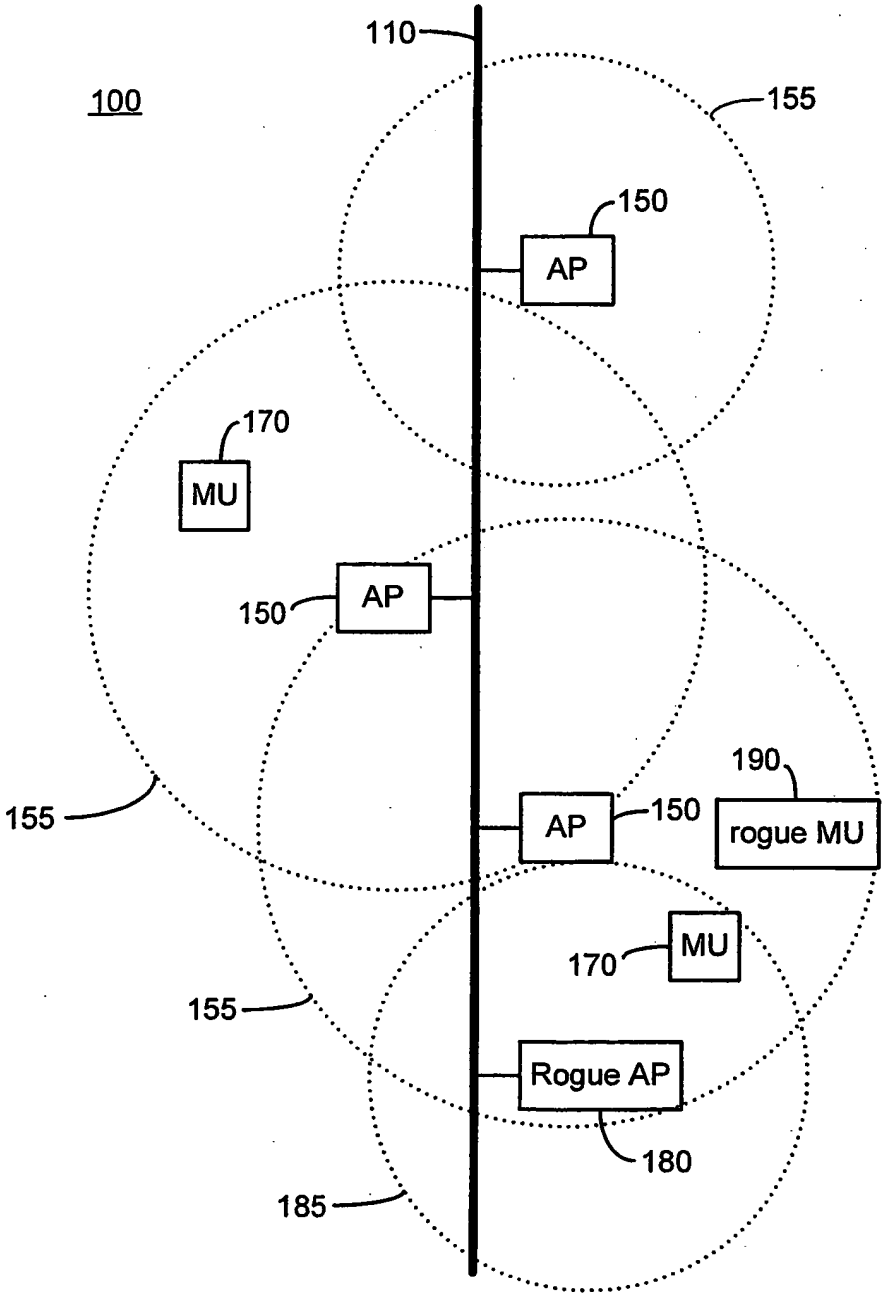

100
110
155
150
AP
170
MU
150
AP
155
190
AP
150
rogue MU
170
MU
155
Rogue AP
180
185

Fig. 1

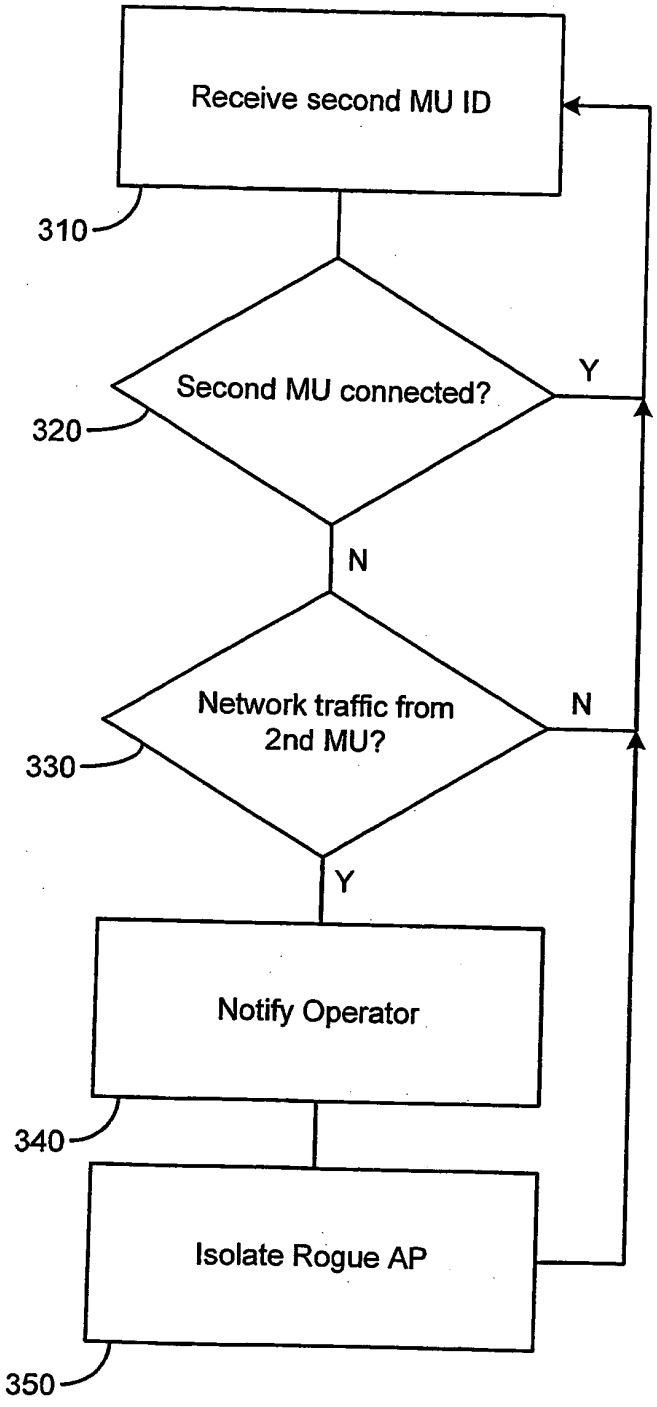



Fig. 3

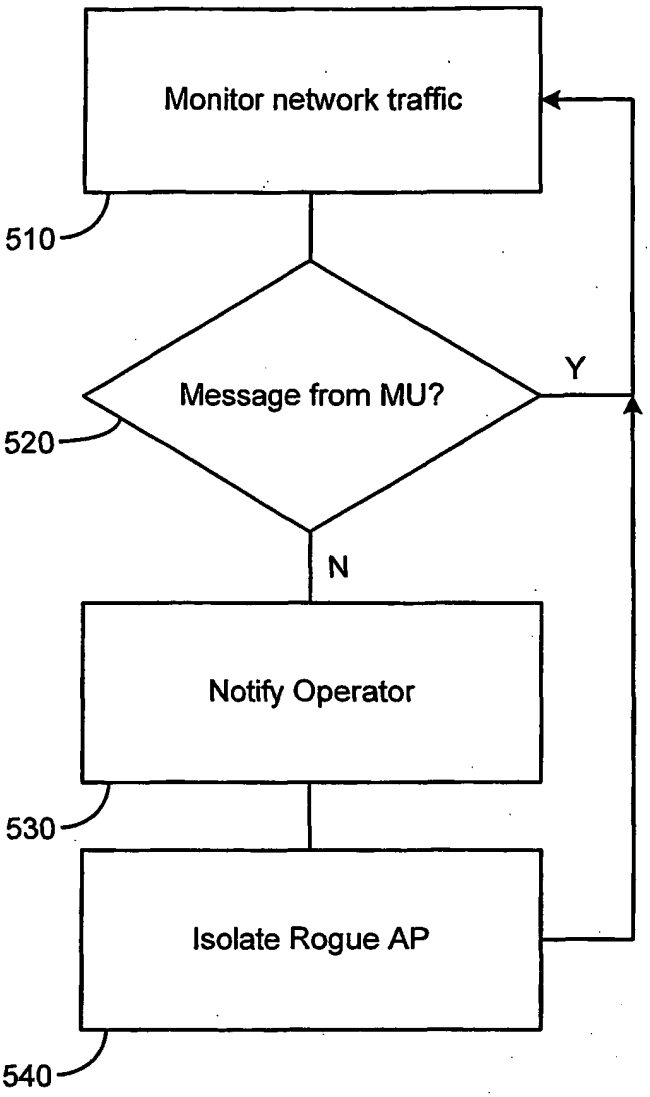

Monitor network traffic
510
Message from MU?
520
Y
N
Notify Operator
530
Isolate Rogue AP
540

Fig. 5

# INTERNATIONAL SEARCH REPORT

Internatio pplication No
PCT/US 03/20502

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | IBM: "IBM Researchers Demonstrate Industry's First Self-diagnostic Wireless Security Monitoring Tool " IBM RESEARCH NEWS , 'Online! 17 June 2002 (2002-06-17), page 1 XP002263356 HAWTHORNE, N.Y Retrieved from the Internet: <URL:http://www.research.ibm.com/resources /news/20020617_dwsa.shtml> 'retrieved on 2003-11-28! the whole document --- | 1-13 |
| X | IBM: " IBM Research Demonstrates Industry's First Auditing Tool For Wireless Network Security " IBM RESEARCH NEWS , 'Online! 12 July 2001 (2001-07-12), page 1 XP002263357 HAWTHORNE, N.Y Retrieved from the Internet: <URL:http://www.research.ibm.com/resources /news/20010712_wireless.shtml> 'retrieved on 2003-11-28! the whole document ----- | 1,4-9,12 |

Form PCT/ISA/210 (continuation of second sheet) (July 1992)